

# Setting expectations: Social networking at work

Personal use of social networking by employees—both on the job and off the clock—can cause major headaches for employers who fail to take the proper precautions.

by Jeffrey T. Cox and Kelly M. Rethman





In this digital era, timeworn notions of client development and prospecting for business have been complemented (many argue, supplanted) by the advent of new online social media and networking opportunities. Once, the cultivating of business relationships might have been most routinely affected by the swapping of business cards while exchanging war stories over cocktails or after a heated battle on the golf course. Now add online social networking to the arsenal. For those less tech-savvy, “[o]nline social networking is the practice of using a Web site or other interactive computer service to expand one’s business or social network.”<sup>1</sup> Once merely a convenient way to keep in touch with friends and family, online social networking sites have become one of the easiest—and some contend, most effective—methods of building business relationships.

Some of the most popular social networking websites include LinkedIn, Facebook, Twitter and MySpace.<sup>2</sup> LinkedIn, with more than 85 million members, is the most business-oriented of the three.<sup>3</sup> LinkedIn allows its users to manage information publicly available about them as professionals, to find and be introduced to potential clients, to get in touch with former classmates and colleagues and even to find qualified job applicants.<sup>4</sup> With business awaiting amidst one’s online connections, executives and employees from all the Fortune 500 companies are using on-

line professional development and business prospecting opportunities via the Web.<sup>5</sup>

#### Social networking poses risks to employers

The benefits of online social networking, however, do not come without attendant risks. Accordingly, employers (and their employees) must be mindful of the power of the Internet to spread news—good or bad—at light speed. All employees, not just executives, have access to and use online social networking websites. Consequently, a lot of information sharing can, and routinely does, occur without the employer having knowledge of the employee’s use of the social networking site, let alone the contents of the information the employee has posted. Others can view the information through a connection or by an Internet search of an employee with non-private profile settings. Even if the employee has used private profile settings, an inquisitive, motivated user of a social networking tool may still be able to obtain the desired information through other means. Thus, the information could be available to the employer’s competitors, government regulators, the employee’s coworkers, potential new employees, prospective customers or business partners. It is easy to see how an employee’s use of online social networking could potentially become quick trouble for an employer.

One of many risks to consider is that the information posted to online social net-

working websites could be used as evidence in litigation against an employer. Not only can an employer’s information get into the wrong hands, but even worse, an employer may face an enhanced risk of civil liability exposure based on the content of information provided by an employee on his or her social networking account. For instance, a LinkedIn account often provides the user’s employer, the user’s position with such employer and frequently the types of duties that position entails. While the law in this regard continues to develop, courts may construe this information as evidence that the employee is acting as an agent of the employer, which means the employer could be liable for the actions of the employee.<sup>6</sup> Thus, the use and content of an employee’s social networking site may become the liability of his or her employer. For example, an employee who unintentionally (or intentionally) discloses insider information on his or her online networking tool might readily create SEC liability for his employer. Similarly, an employer bears the risk of liability for an employee’s blog statements if the content of the blog includes defamatory statements about another and blogging is one of that employee’s job responsibilities.<sup>7</sup> The list does not end with potential disclosure of insider information or the risk of defamatory, embarrassing or inappropriate content. Consider the following scenarios.

- After completing a long, stressful shift, a nurse makes a Facebook status update

that inadvertently discloses confidential medical information, creating liability for the hospital employing her.

- A proud employee copies material from a recent news article about one of his employer’s recent successes, pastes it into his LinkedIn site and, instead of passing along good press, the employee unintentionally creates a copyright infringement liability risk for his employer.
- An employee posts explicit material on her MySpace page, or even on a co-worker’s page, that might be deemed sexually harassing or lewd and inappropriate content, creating not only employer liability, but also a poor work environment.
- An engineer, excited about a recent business development, “tweets” confidential trade secret information, making that information public and no longer a protectable trade secret for his employer.
- A salesperson, trying to build professional connections on behalf of her employer, makes social networking connections with all of her customers, making her list of contacts on that site the equivalent of a public customer list that is no longer a protectable trade secret for her employer.<sup>8</sup>
- A new employee puts up a Facebook post about how great his employer’s new product is without disclosing his connection with the employer, and without intending to, simultaneously dunks his new employer in Federal Trade Commission hot water regarding employee endorsements, or exposes his new employer to the prospect of false advertising litigation.
- An employee of a small business bringing a Title VII discrimination claim points to another employee’s LinkedIn account that lists her employer’s integration with a larger company as evidence that the employer employs at least 15 employees, thus incurring Title VII liability.<sup>9</sup>
- An employer files a motion to transfer the venue of a case to California, which it alleges is the principal place of business of the company, but the opposing party points to an executive’s social networking account that lists her employer’s place of business as Florida as a reason for the court to deny the motion.<sup>10</sup>

#### Solutions for employers

What can employers do to prevent themselves from potential online social networking disasters? In addition to taking care to effectively plan, communicate and enforce company policies regarding the use of such networking tools, employers should take a critical look at reshaping their employment contracts. Employment contracts addressing the use of social networking sites provide two major advantages over those silent on the issue. “By articulating permitted and prohibited activities, a company may be able to establish its ‘good faith,’ and demonstrate that certain employee activities were outside the course and scope of employ (thereby avoiding imputed liability for the employees’ actions).”<sup>11</sup> Indeed, an employment contract clearly setting forth the parameters of the employee’s use of social networking sites provides a useful aid in defense of a wrongful termination suit that might occur after the employer terminates the employee for using a site against the terms of the contract.<sup>12</sup>

There are several categories of information that employers should focus on when re-vamping employment contracts to address online social networking.

#### Content

The employment contract should set forth what information employees are and are not allowed to make public. Specifically, the contract should address the disclosure of confidential information, as well as the posting of defamatory, copyright protected and potentially sexually harassing material. The contract might also emphasize the use of common sense and good judgment when using social media in a way that affects the company, its customers or its employees.

#### Administrative

Employment contracts should also discuss some of the administrative aspects of social networking. This includes the hours when the use of social networking sites is acceptable and whether the employees may or should use their work email when registering their accounts.

#### Disclaimer

The employment contract should state whether the employee needs to post a disclaimer or make certain disclosures to differentiate information posted as an agent of the employer versus information outside the employment relationship.

#### Right to monitor

While potentially a hot button issue in this era of mobile communication devices where the lines of work and leisure time are blurred, the employment contract might reserve the right of the employer to monitor employee use of social media while at work or while using employer issued electronic devices.

#### Penalties for breach

Employment contracts should also address the repercussions of breaching the contract. What are the rights and damages available in the event of breach? Under what circumstances would termination of employment be an appropriate sanction? The contract should also include the right to hold employees accountable for use of their personal devices, and while on non-work time where the company’s business interests are implicated.

Employers certainly should consider how best to use employment contracts to define the employee’s social networking activities. An employer has a legitimate interest in and can address long-term customer relationships, goodwill and proper treatment of general confidential information.<sup>13</sup> Additionally, employees owe other employees the duty to not defame, harass or intimidate.<sup>14</sup>

As with any employment contract, however, the terms addressing social networking should not go as far as to impinge on other employee rights. Generally, private employers have much greater freedom to restrict or inhibit an employee’s workplace communications.<sup>15</sup> Indeed, in a carefully watched U.S. Supreme Court decision, *City of Ontario v. Quon*, the Court affirmed that employers should also have little angst about rights to online privacy, as employees are unlikely to have a reasonable expectation of privacy in social media communications.<sup>16</sup> In *Quon*, an employer (the city) obtained and reviewed the transcript of the employee’s pager messages, and the employee brought suit that the employer violated his Fourth Amendment rights of privacy.<sup>17</sup> The Court found that the search was reasonable because “the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification.”<sup>18</sup> The Court noted that the search would have been regarded as reasonable in the private employer context as well, and specifically noted that “employer policies concerning communications will of

course shape the reasonable expectations of their employees.”<sup>19</sup>

However, many employees do have a right to whistle blow and protest, and employment contracts should preserve those rights.<sup>20</sup> Further, to be mindful of off-duty lawful activity laws, employment contracts should always have a nexus between the employee’s actions or conduct and his or her job performance, the employer’s product or reputation or another legitimate business reason.<sup>21</sup>

### Proactively address employee use of online social networking

The caution for employers is to appreciate and take advantage of the business development and enhanced marketing value social networking sites offer (competitors surely are), while also keeping in mind the inherent risks of the tools. Employers must recognize that their employees are—unquestionably—using social networking sites and, to avoid or at least minimize business and legal risks, employers should carefully consider implementing (or revising) employment contracts to address specifically permitted and prohibited social networking use. Employers cannot ignore the risks social networking sites pose, and must instead protect their confidential information, reputation and trade secrets through all available means; one of the best starting points is an assessment and updating of their employment contracts. ■

### Author bio



Jeffrey T. Cox is a partner and Kelly M. Rethman an associate with Faruki Ireland & Cox P.L.L., a national complex trial and litigation boutique with offices in Cincinnati and Dayton. Cox can be reached at jcox@ficlaw.com and Rethman can be reached at krethman@ficlaw.com.



### Endnotes

<sup>1</sup> *Doe v. MySpace Inc.*, 528 F.3d 413, 415 (5th Cir.), cert. denied, 129 S. Ct. 600 (2008).  
<sup>2</sup> Facebook allows its users to create user profiles, including personal information, their interests and photographs, all of which can be shared

with other Facebook “friends.” *Facebook, Inc. v. Power Ventures, Inc.*, No. 08 5780, 2009 U.S. Dist. LEXIS 42367, at \*3 (N.D. Cal. May 11, 2009). Similarly, MySpace users create personal profiles and communicate with other users through email, instant messaging and blogs. *Doe*, 528 F.3d at 415.

<sup>3</sup> As an example, LinkedIn allows its users to create profiles that summarize their professional expertise and accomplishments. After users create their profiles, users can form “connections” with other professionals they know. Once a user connects with another professional, the user is automatically linked to that professional’s connections as well. Thus, a network is formed that consists of the user’s connections as well as the user’s connections’ connections, such that each user is linked to a vast number of other professionals and experts. LinkedIn “About Us” page, <http://press.linkedin.com/about> (last visited Jan. 3, 2011).

<sup>4</sup> LinkedIn “About Us” page, <http://press.linkedin.com/about> (last visited Jan. 3, 2011).

<sup>5</sup> *Id.*

<sup>6</sup> *Park West Galleries, Inc. v. Hochman, Nos. 08 12247; 08 12274*, 2010 U.S. Dist. LEXIS 12488 (E.D. Mich. Feb. 12, 2010) (third party claimed the employer’s employees made defamatory statements about it; in determining whether an agency relationship existed between the employer and its employees that allegedly made the defamatory statements, the court examined the employees’ LinkedIn accounts and ultimately denied the employer’s motion for summary judgment after finding remaining issues of fact).

<sup>7</sup> *Id.*

<sup>8</sup> *Softchoice Corp. v. MacKenzie*, 636 F. Supp. 2d 927, 933 (D. Neb. 2009) (employer brought a trade secret and unfair competition claim alleging that an ex-employee used its customer list in his new employment; the court granted summary judgment in favor of the ex-employee after finding the customer list could be obtained through multiple public sources, including “membership in social networks such as ‘LinkedIn.com’”).

<sup>9</sup> *Freire v. Keystone Title Settlement Servs., Inc.*, No.08 2976, 2009 U.S. Dist. LEXIS 121190 (D. Md. Dec. 29, 2009) (employee alleged that her employer discriminated against her in violation of Title VII; the employer defended itself by arguing Title VII was inapplicable because it had less than 15 employees; the court agreed with the employer and granted summary judgment in its favor after examining another employee’s LinkedIn account that made no showing that the employer was integrated with any other corporations and concluding that the employer employed less than 15 employees), *aff’d*, No. 10 1126, 2010 U.S. App. LEXIS 15817 (4th Cir. July 29, 2010) (per curiam).

<sup>10</sup> *Autodesk Can. Co. v. Assimilate, Inc.*, No. 08 587, 2009 U.S. Dist. LEXIS 89794, at \*10

(D. Del. Sept. 29, 2009) (plaintiff argued against defendant’s motion to transfer venue from Delaware to California by noting that plaintiff’s “LinkedIn profile list[ed] its principal place of business as Florida”). Accord: *Safco Prods. Co. v. Welcom Prods., Inc.*, No. 08 4918, 2010 U.S. Dist. LEXIS 80581 (D. Minn. Aug. 2, 2010) (denying defendant’s motion to dismiss the patent suit against it based on lack of personal jurisdiction after finding defendant’s LinkedIn account stated that it provided products to companies that were headquartered in Minnesota).

<sup>11</sup> *Employee Use of the Internet and Email: A Model Corporate Policy 1* (David M. Doubilet and Vincent I. Polley eds., American Bar Association, 2002). While not from the social networking sphere, traditional benefits of well-grounded employment contracts apply. *Fraioli v. Lemcke*, 328 F. Supp. 2d 250, 271 (D. R.I. 2004) (employee defrauded and embezzled more than \$1 million from plaintiffs, and plaintiffs brought various negligent supervision, fraud, securities, investing and embezzling claims against the employee and his employer under the doctrine of respondeat superior; the court granted summary judgment in favor of the employer after finding that the employee’s actions “were beyond the scope of his employment agreement”); *Viado v. Domino’s Pizza, LLC*, 217 P.3d 199, 212 (Or. Ct. App. 2009) (plaintiff was injured in a collision with a delivery truck operated by a franchisee employee, and the plaintiff brought a negligence suit against the franchisor under the theory that the franchisor should be vicariously liable for the franchisee employee’s actions; the court affirmed summary judgment in favor of the franchisor after finding that the franchise agreement provided that the franchisee “control[led] the day to day performance of its delivery drivers, and that [the franchisor] ha[d] no right to control the conduct of those drivers”).

<sup>12</sup> *Marshall v. Mayor of Savannah*, No. 09 13444, 2010 U.S. App. LEXIS 3233 (11th Cir. Feb. 17, 2010) (per curiam) (employer had a policy regarding using names and pictures to endorse products, employee posted the employer’s pictures alongside nude pictures of herself on her MySpace page and the employer subsequently terminated her on the basis of her violation of the contract; the court affirmed summary judgment in favor of the employer on the employee’s Title VII and §1983 claims).

<sup>13</sup> Mark Filipp, *Covenants Not to Compete* §3.01, at 3-3 (Wolters Kluwer 3d ed. Supp. 2010).

<sup>14</sup> Richard A. Paul and Lisa Hird Chung, “Brave New Cyberworld: The Employer’s Legal Guide to the Interactive Internet,” *24 Lab. Law*. 109 (2008).

<sup>15</sup> *Pietrylo v. Hillstone Rest. Group*, No. 06 5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 24, 2008) (employees had a MySpace group regarding their employer, the employer gained access to the group through another employee and the plaintiffs were subsequently

terminated; the court granted the employer’s motion for summary judgment on the employees’ freedom of speech claim because the employer was a private employer and the employees’ speech was not of public concern). Accord: Thompson’s HR Policies 373 (Thompson 2008) (“While employees have the right to speak their mind on their own time, a private employer—who is not subject to the First Amendment—can regulate who speaks on behalf of the company, what information is conveyed and the tone of the message.”)

<sup>16</sup> *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

<sup>17</sup> *Id.* at 2626.

<sup>18</sup> *Id.* at 2633.

<sup>19</sup> *Id.* at 2630; *Pack v. Wood County*, No. 08 cv 198, 2009 U.S. Dist. LEXIS 57103 (E.D. Tex. July 30, 2009) (an individual’s co-employees remotely accessed the employee’s computer hard drive and supplied the allegedly pornographic files they found to authorities, and the employee whose computer was searched brought suit against his employer for violation of his right to be free from an unreasonable search; the court granted the employer’s motion for summary judgment after finding the employee had no expectation of privacy in his office computer’s hard drive because his employer owned the computer that transmitted or stored the communications and the computer was supplied

to the employee for work purposes). Accord: Alan J. Bojorquez & Damien Shores, “Open Government and the Net: Bringing Social Media Into the Light,” *11 Tex. Tech. Admin. L. J.* 45, 67 (2009) (“Employees generally have little or no expectation of privacy regarding electronic data, such as e mails, particularly those transmitted through the employer’s network.”)

<sup>20</sup> 5 U.S.C.S. §2302(b) (“Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority . . . (8) take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because of (A) any disclosure of information by an employee or applicant which the employee or applicant reasonably believes evidences (i) a violation of any law, rule, or regulation, or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety . . . .”); *O’Hare Truck Serv. v. City of Northlake*, 518 U.S. 712, 723, 116 S. Ct. 2353, 2360 (1996) (“Independent contractors, as well as public employees, are entitled to protest wrongful government interference with their rights of speech and association.”) Accord: Marvin F. Hill, Jr. and James A. Wright, *Employee Lifestyle and Off Duty Conduct Regulation*, at 21 (BNA 1993) (an employee has the common law right to whistle blow about his su-

pervisor’s conduct and the company’s activities, but “the conduct complained of must be clearly illegal”).

<sup>21</sup> N.Y. Labor Law §201-d(2) (Consol. 2010) (“Unless otherwise provided by law, it shall be unlawful for any employer or employment agency to refuse to hire, employ or license, or to discharge from employment or otherwise discriminate against an individual in compensation, promotion or terms, conditions or privileges of employment because of: . . . c. an individual’s legal recreational activities outside work hours, off of the employer’s premises and without use of the employer’s equipment or other property . . . .”); Col. Rev. Stat. 24-34-402.5(1) (2010) (“It shall be a discriminatory or unfair employment practice for an employer to terminate the employment of any employee due to that employee’s engaging in any lawful activity off the premises of the employer during nonworking hours . . . .”). Accord: Brian M. Molinari, “When Online Behavior Becomes a Real World Problem,” *N.Y. Emp. L. Letter* (Sept. 2009) (noting that off duty lawful activity statutes often afford “no protection to an employee whose off duty conduct ‘creates a material conflict of interest related to the employer’s trade secrets, proprietary information or other proprietary or business interest.’”) quoting N.Y. Labor Law §201 d.

